CLAIMS

What is claimed is:

1. A method comprising:

provisioning a symmetric cryptographic key across multiple clients through multiple embedded agents, each client having one of the embedded agents, one embedded agent in each client having an embedded agent to store the symmetric cryptographic key in a storage accessible to the embedded agent and not directly accessible to a host processor on the client; and

providing access to an encrypted traffic flow in a network to a client if the client is authenticated with the key.

2. A method according to claim 1, wherein provisioning the key through the embedded agents further comprises provisioning the key through an embedded agent having network access via a network link not visible to a host operating system (OS) running on the client.

3. A method according to claim 2, wherein providing access to the traffic flow if the client is authenticated comprises the embedded agent authenticating the client over the network line not visible to the host OS.

4. A method according to claim 1, wherein providing access to the traffic flow further comprises providing multiple clients access with the key to nodes in the network, the nodes in the network to decrypt the traffic flow and subsequently encrypt the traffic flow to transmit the traffic to a next node in the network.

5. A method according to claim 1, further comprising updating at a client the symmetric cryptographic key provisioned across the multiple clients through a public and private key exchange with a public and private key associated the client.

6. A method according to claim 1, wherein providing access if the client is authenticated further comprises:

the embedded agent verifying that a platform associated with the client is not compromised; and

the embedded agent providing the key and an assertion that the client is not compromised to a verification entity on the network.

7. A method according to claim 6, further comprising the embedded agent indicating to a remote network device if the client is compromised.

8. A method according to claim 6, further comprising the embedded agent foreclosing network access to the client if the client is compromised.

9. A method according to claim 1, further comprising the embedded agent performing cryptographic functions on data with the key to authenticate data with the key.

10. A method according to claim 1, further comprising the embedded agent including a derivative of the key in a header of data to be transmitted to authenticate the data with the key.

11. An apparatus comprising:

a host platform on the apparatus including a host processor;

a secure memory not visible to applications and an operating system (OS) running on the host platform; and

an embedded computational device communicatively coupled with the host platform, the embedded device to have a network link transparent to the OS, the embedded device to manage a cryptographic key shared among the apparatus and network endpoints to be used to communicate with a server over the network, to receive the cryptographic key on the transparent link and authenticate the apparatus, and to store the cryptographic key in the secure memory.

12. An apparatus according to claim 11, wherein the embedded device to have transparent network link comprises the embedded device to have a network connection not accessible by the host platform, the link to comply with the transport layer security (TLS) protocol.

13. An apparatus according to claim 11, wherein the embedded device to have a transparent network link comprises the embedded device to have a network connection not accessible by the host platform, the link to comply with the secure sockets layer (SSL) protocol.

14. An apparatus according to claim 11, wherein the embedded device to authenticate the apparatus comprises the embedded device to verify the identity of the apparatus to a network switching device with the key, the key to also be used by the network endpoints to verify their respective identities to the network switching device, and the network switching device to decrypt encrypted traffic from the apparatus and the network endpoints.

15. An apparatus according to claim 11, wherein the embedded device to authenticate the apparatus comprises the embedded device to hash traffic to be transmitted with the key.

16. An apparatus according to claim 11, wherein the embedded device to authenticate the apparatus comprises the embedded device to perform cryptographic services with the key on traffic to be transmitted.

17. An apparatus according to claim 11, wherein the embedded device to authenticate the apparatus comprises the embedded device to include a derivative of the key in a header of traffic to be transmitted.

18. An apparatus according to claim 11, further comprising a second embedded computational device, the second embedded device integrated on the host platform, to verify the security of the host platform.

19. An apparatus according to claim 18, wherein the first embedded device does not authenticate the apparatus if the second embedded device determines the host platform is not secure.

20. An apparatus according to claim 18, further comprising a bi-directional private bus between the first and second embedded devices.

21. An apparatus according to claim 11, further comprising a counter mode hardware cryptographical module on the host platform to encipher traffic with the cryptographic key and further provide a counter mode enciphering of the enciphered traffic.

22. A system comprising:

a host platform including a host processor;

a digital signal processor (DSP) coupled with the host platform; and

an embedded chipset including a secure key storage module to perform cryptographic key management of a shared cryptographic key with the secure key storage module and a private communication channel accessible to the chipset and not the host platform, and to access the image of the host platform on the flash to determine the integrity of the host platform, the shared cryptographic key to be used by the host platform to encipher data and other networked devices within a virtual private network.

23. A system according to claim 22, wherein the embedded chipset to perform cryptographic key distribution with the private communication channel comprises the embedded chipset to perform cryptographic key distribution with a communication channel complying with the transport layer security (TLS) protocol.

24. A system according to claim 22, wherein the embedded chipset comprises an embedded controller agent and an embedded firmware agent, the firmware agent to determine the integrity

of the host platform, and the controller agent to operate the private communication channel and manage access by the host platform to secure network connections.

25. A system according to claim 24, further comprising a bi-directional private communication path between the first and second embedded devices to allow the devices to interoperate outside the awareness of the host platform.

26. A system according to claim 22, further comprising the embedded chipset to hash traffic to be transmitted with the key to authenticate the system to one of the other networked devices.

27. A system according to claim 22, further comprising the embedded chipset to perform cryptographic services with the key on traffic to be transmitted to authenticate the system to one of the other networked devices.

28. A system according to claim 22, further comprising the embedded chipset to include a derivative of the key in a header of traffic to be transmitted to authenticate the system to one of the other networked devices.

29. An article of manufacture comprising a machine accessible medium having content to provide instructions to cause a machine to perform operations including:

provisioning a symmetric cryptographic key across multiple clients through multiple embedded agents, each client having one of the embedded agents, one embedded agent in each client having an embedded agent to store the symmetric cryptographic key in a storage accessible to the embedded agent and not directly accessible to a host processor on the client; and

providing access to an encrypted traffic flow in a network to a client if the client is authenticated with the key.

30. An article of manufacture according to claim 29, wherein the content to provide instruction to cause the machine to perform operations including provisioning the key through

the embedded agents further comprises the content to provide instruction to cause the machine to perform operations including provisioning the key through an embedded agent having network access via a network link not visible to a host operating system (OS) running on the client.

31. An article of manufacture according to claim 31, wherein the content to provide instruction to cause the machine to perform operations including providing access to the traffic flow if the client is authenticated comprises the content to provide instruction to cause the machine to perform operations including authenticating the client with the embedded agent over the network line not visible to the host OS.

32. An article of manufacture according to claim 29, wherein the content to provide instruction to cause the machine to perform operations including providing access to the traffic flow further comprises the content to provide instruction to cause the machine to perform operations including providing multiple clients access with the key to nodes in the network, the nodes in the network to decrypt the traffic flow and subsequently encrypt the traffic flow to transmit the traffic to a next node in the network.

33. An article of manufacture according to claim 29, further comprising the content to provide instruction to cause the machine to perform operations including updating at a client the symmetric cryptographic key provisioned across the multiple clients through a public and private key exchange with a public and private key associated the client.

34. An article of manufacture according to claim 29, wherein the content to provide instruction to cause the machine to perform operations including providing access if the client is authenticated further comprises the content to provide instruction to cause the machine to perform operations including:

verifying with the embedded agent that a platform associated with the client is not compromised; and

providing with the embedded agent the key and an assertion that the client is not compromised to a verification entity on the network.

35. An article of manufacture according to claim 34, further comprising the content to provide instruction to cause the machine to perform operations including indicating with the embedded agent to a remote network device if the client is compromised.

36. An article of manufacture according to claim 34, further comprising the content to provide instruction to cause the machine to perform operations including foreclosing with the embedded agent network access to the client if the client is compromised.

37. An article of manufacture according to claim 29, further comprising the content to provide instruction to cause the machine to perform operations including performing cryptographic functions on data with the key to authenticate data with the key.

38. An article of manufacture according to claim 29, further comprising the content to provide instruction to cause the machine to perform operations including placing a derivative of the key in a header of data to be transmitted to authenticate the data with the key.